

**TF-AACE Meeting
Malaga 21 November 2003**

Agenda

1. Opening
2. Root CA collection: TACAR
3. Status of the task-force and deliverables. Future activities of TF-AACE (if any)

1. Opening

A short TF-AACE was held after the workshop in Malaga. Most of the meeting was focused about TACAR and the collection of certificates started.

2. TACAR

After discussions on the mailing, the TACAR policy document was presented by Diego Lopez and discussed for the time with all the participants. The overall procedure was defined a bit more complicated than it was expected and some amendments to the document, described below, were required:

1. the policy document foresaw in a first moment that the ID number used for the identification of the applicants were stored in the document. This was changed. No ID number will be registered in the documents
2. there were some inconsistencies between what described in the policy and the template of the registration/accreditation letters
3. an explanation of some terms used was required

The use of the PGP was discussed. PGP keys are used (in case the applicants decide to follow the accreditation procedure) to amend/update the documents. In case PGP keys are not provided the amendment will be done via face-to-face meeting or snail mail.

Chelo Malagon and Diego Lopez have changed to policy document to include the changes required. The policy is now on-line and it is currently used.

4. Status of the task-force. Future activities of TF-AACE (if any)

AA-RR

Diego made a presentation about the idea of defining and building a requester/responder (SAML-RR) able to use some metadata describing the requirements of some infrastructure in order to validate (or make at least an initial assessment on) the interoperability of some component with other(s).

The SAML-RR will be built on the following assumptions:

- 1) The number of different components, systems, APIs, etc. able to run into AA interactions seems to be much greater in the near future, as other application domains become aware of available technologies and their potential benefits. In many cases, existing procedures or specific constraints will drive to the establishment of "local" solutions that should be able to interoperate with national, international, or trans-national initiatives.

- 2) These components are going to operate at different levels upon the network infrastructure (and even inside), so many of the assumptions about software architecture, languages, etc. will not hold in a significant number of cases.
- 3) As it has been widely recognized, different infrastructures (supported by federations, virtual organizations, or whatever you name them) are going to have different requirements on which attributes and values are to be requested and/or enforced.

The SAML RR will be able to use external definitions to simulate the external behaviour of different components of several infrastructures in order to assess the interoperability of a certain element with them. The SAML RR will be able to learn from those elements it connects to, enhancing its knowledge base.

Diego presented three types of components that the SAML RR would be able to impersonate:

- 1) Attribute sources (like a Shibboleth AA, a A-Select server, a PAPI AAAS, or an Athens XAP). These are, essentially, entities able to accept Attribute queries from entities of type 2) and respond with attribute information.
- 2) Attribute Requesters (like a Shibboleth SHAR, a VOMS server, a PAPI PoA, or a Athens DSP entry point). These entities perform requests about user attributes to entities of type 1) and make an authorization decision on them, possibly querying an entity of type 3).
- 3) Authorization Engines (like Permis or SPCOP). These entities make decisions from the requests they receive from entities of type 2) and their internal configuration. They return a simple (yes/no) or complex (for example, a SPOCP "blob") answer to the query.

Diego said that the SAML RR should follow these steps:

- 1) Define a (set of) SAML interoperable profile(s). This is something we more or less agree to do in the Amsterdam developer meeting, although not very much has been done. The profile(s) will be, at least, applied to the SOAP/HTTP binding.
- 2) Define a way for describing and storing which profiles and attributes are required or provided by a certain component. I think we can either use RDF for this or take advantage of Peter Gietz's work on LDAP schemas.
- 3) Implement the requester/responder using openSAML (as also agreed in Amsterdam), and make it available (at least) as a SOAP service over HTTP.

Diego's presentation was warmly welcomed. It was agreed to make the RR protocol independent and consider some other protocols like SPOCP, thus the name of the system itself was changed from SAML-RR to AA-RR.

ACTION: RedIRIS to start with a more detailed design of the system architecture, and to evaluate different ways for profile definition.
SWITCH to help with this.

Future of the task force

The future of the task force was discussed, also in relation to GEANT2, which was talked about during the workshop. A first possibility was to merge TF-AACE and TF-mobility, but because TF-AACE is a bit different in terms of practical results from TF-Mobility joining the two groups was not considered a good idea.

Another and better proposal was to have a wider task-force to discuss middleware issues, a sort of forum to discuss new ideas and running projects, resembling more TF-CSIRT. This idea got a lot of consensus.

In case of TF-AACE follow up, it was also agreed that this new group and TF-Mobility would hold one joint event per year (which will be attended by JRA5 members as well) to discuss overlapping issues and present their work. It was also proposed that each group should have a member from the other group actively involved to ensure good communications are in place between both groups.

ACTION: to prepare a draft charter for the new TF-AACE for the next TNC.

Summary

All the actions are closed by now, a part from the AA-RR, which is expected to be ready shortly and presented during the next TERENA Conference and the preparation of the new Terms of Reference of the task-force.

Attendees

Carsten Bormann	Universitaet Bremen TZI
Marco Casassa Mont	Hewlett-Packard laboratories
Rodrigo Castro	RedIRIS
Sally Chambers	University of London
David Collados	Caltech
Dimitris Daskopoulos	GRNET
Mijo Derek	SRCE
Licia Florio	TERENA
Tony Genovese	ESnet/LBNL
Brian Gilmore	The University of Edinburgh
Victoriano Giralt	University of Malaga
Isabel Barroso Gomez	University of Oslo
Roland Hedberg	Stockholm University
Michael Helm	ESnet/LBNL
David Kelsey	CCLRC-RAL
Ueli Kienholz	SWITCH
Mikael Linden	Funet/CSC
Diego Lopez	RedIRIS
Javier Lopez	University of Malaga
José Manuel Macías	RedIRIS
Chelo Malagón	IRIS-CERT, RedIRIS
Rafael Marco de Lucas	Instituto de Fisica de Cantabria (IFCA-Spain)
Ingrid Melve	Uninett
Miroslav Milinovic	SRCE
Juan J. Ortega	University of Malaga
Anand Patil	DANTE

Dubravko Penezic
Janis Pinkis
Jürgen Rauschenbach
Alan Robiette
Nicolas Simar
Jarmo Sorvari
Milan Sova
Chris van der Merwe
Torbjorn Wiberg

SRCE
University of Latvia
DFN-Verein
JISC
DANTE
Tampere Polytechnic
CESNET
Arnes
Umeå Universitet